Trigger Violations Against Common Policies with Sample Data

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Examples

- ABA Routing Numbers
- US Family Educational Rights and Privacy Act
- Credit Card Numbers
- Driver License Numbers
- US Sarbanes-Oxley
- National Provider Identifiers
- Social Security Numbers

Related Information

Introduction

This document describes sample data that can be used to test Data Loss Prevention (DLP) policies in order to confirm that they work as intended.

Prerequisites

Requirements

Cisco recommends that you have the DLP feature key installed and in use.

Components Used

The information in this document is based on these software and hardware versions:

- ESA that runs AsyncOS 11.x or later.
- DLP engine 1.0.18.d7b4601 or later (can be obtained with the **dlpstatus** command from the CLI).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Examples

In order to utilize the sample data, complete these steps:

1. Create the DLP policy (for example, American Banking Association (ABA) Routing Numbers) and attach it to an Outgoing Mail Policy.
2. Choose **Submit > Commit** in order to commit the changes.
3. Send an email through the ESA which hits the newly created DLP policy on the Outgoing Mail Policy it was applied to.
   The test email must include the sample data, which can be placed in the body (for example, ABA Routing Number: 800000080).
4. Review the mail logs or Message Tracking in order to confirm that a DLP violation had occurred.

ABA Routing Numbers

- **Policy Description:** Identifies ABA routing numbers.
- **Policy Matching Details:** Identifies ABA routing numbers, issued for banks in the United States.
- **Sample Data:** ABA Routing Number: 800000080.

US Family Educational Rights and Privacy Act

- **Policy Description:** Identifies information protected by the Family Education Rights and Privacy Act (FERPA).
- **Policy Matching Details:** This policy identifies Social Security numbers, student records, and optional custom student numbers.
- **Sample Data:** M.Ed. Magic, University of Wizardry; Course Units Grade MATH 1A 3.0 A+ CHEM 1B 3.0 B ARTS 1C 2.0 A; Fall Semester Course Numbers: CHEM101, ECON102, MATH103.

Credit Card Numbers

- **Policy Description:** Identifies credit card numbers from major issuers.
- **Policy Matching Details:** Matches contextual numbers from issuers such as American Express, Diners Club, Discover, JCB, Mastercard, VISA, and China UnionPay.
- **Sample Data:** 5424-5224-5424-5226 Exp. Date: 05/2018.

Driver License Numbers

- **Policy Description:** Identifies driver license numbers issued in the United States.
- **Policy Matching Details:** Identifies driver license numbers issued in the United States.

- **Sample Data:** MN DL# L899999999998; DL# 899999998.

US Sarbanes-Oxley

- **Policy Description:** Identifies information protected by the Sarbanes-Oxley (SOX) Act.
- **Policy Matching Details:** This policy searches for financial documents.
- **Sample Data:** Gross Profits, Current Assets, and Cash Flow Statement for the Quarter ended June 30, 2016.

National Provider Identifiers

- **Policy Description:** Identifies National Provider Identifiers (NPIs) issued in the United States.
- **Policy Matching Details:** Identifies NPIs issued in the United States.
- **Sample Data:** NPI No. 1235678996; NPI No. 808401235678996.

Social Security Numbers

- **Policy Description:** Identifies social security numbers (SSNs) issued in the United States.
- **Policy Matching Details:** Identifies formatted and unformatted SSNs issued in the United States.
- **Sample Data:** SSN 132-45-6798.

Related Information

- Cisco Email Security Appliance - End-User Guides
- What is Data Loss Prevention?
- Data Loss Prevention - Troubleshooting Misclassifications and Scanning Failures
- Technical Support & Documentation - Cisco Systems